UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,446	06/11/2001	Michael A. Inchalik	82811RLO	2137

7590 01/13/2005

Thomas H. Close
Patent Legal Staff
Eastman Kodak Company
343 State Street
Rochester, NY 14650-2201

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,446	INCHALIK ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☒ Claim(s) *1,3 and 9* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 June 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6-11-01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-15 have been examined and are pending.

Information Disclosure Statement

The IDS submitted by the applicant has been considered by the examiner.

Drawings

1. Figures 1b-1d should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.
2. Figure 4: The drawings are objected to because item 116 is missing from the applicant's numbering scheme. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet,

and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The abstract of the disclosure is objected to because commas are missing from the abstract that cause the comprehension of the abstract to be more difficult than necessary when reading it. There should be a comma after the word "signature" in line 11 and after the word "use" in line 17. Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities:

- Page 6, line 19 should state "FIG. 1a" not "FIG. 1" as "FIG. 1" does not exist among the drawings submitted by the applicant.

Appropriate correction is required.

Claim Objections

Claims 1, 3, and 9 are objected to because of the following informalities: commas are missing that cause the comprehension of the claims to be more difficult than necessary when reading them.

As per claims 1, 3, and 9:

- There should be a comma after "signature" in line 3 of claims 1, 3, and 9, section c.
- There should be a comma after "use" in section e, line 3 of claim 1; section f, line 3 of claim 3; and section f, line 3 of claim 9.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 recites the limitations "the disc" in part b, line 2; "the optical disc" in part c, line 2; "the encoded encrypted information" in part e, lines 3-4; and "the user memory location" in part e, line 4. There is insufficient antecedent basis for these limitations in the claim.
2. Claim 3 recites the limitations "the disc" in part b, line 2; "the optical disc" in part c, line 2; and "the encoded encrypted information" in part f, lines 3-4. There is insufficient antecedent basis for these limitations in the claim.
3. Claim 9 recites the limitations "the disc" in part b, line 4; "the optical disc" in part c, line 2; and "the encoded encrypted information" in part f, lines 3-4. There is insufficient antecedent basis for these limitations in the claim.

4. Any claims not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (U.S. 6,298,441) in view of RFC 2104 ("HMAC: Keyed-Hashing for Message Authentication"), Yamagishi (U.S. 5,379,433), and Richards (U.S. 6,385,723).

1. Claim 1: Handelman et al disclosed a method of transferring information from a content supplier from one or more databases, such information including program(s), audio, still pictures, video, or data files (e.g. lists, spreadsheets, reports, documents, presentation graphics, sales information), or combinations thereof to a location (col 3, lines 9-19) that uses an authorizing hybrid disc that permits the use of such transferred information, comprising the steps of:
    - Providing an authorizing disc having a ROM portion and a RAM portion (col 9, lines 21-27 and col 12, lines 36-54).
    - Providing the ROM portion to include a preformed identification signature which is impressed into the ROM portion of the authorizing

disc and is arranged to be difficult for a pirate to copy (col 4, lines 11-21).

The examiner has interpreted the term "disc" to also include cards. This may include smart cards or integrated circuit cards. It should be noted that the smart card device as disclosed by Handelman et al can make use of a separate memory card which can also be an optical disc (col 9, lines 21-27). Further, Handelman et al later disclose that the memory card and the smart card can be combined into one card/disc (col 12, lines 37-40). In column 4, lines 11-21, Handelman disclosed that a user of a smart card would not be able to receive a document unless they were authorized to do so. Such authorization can only come about through the use of some sort of identification feature encoded within the smart card. The examiner has interpreted any such identification feature as a signature, including passcodes, keys, message authentication codes, or passwords.

The use of hybrid optical discs, which include a RAM and an identification signature located in a ROM portion and is arranged to be difficult for a pirate to copy is also disclosed by Yamagishi (col 2, lines 23-56). One of ordinary skill in the art at the time of the applicant's invention would be motivated to make use of a hybrid optical disc as a smart card because the amount of memory that is available on an optical disc to use as storage for downloaded information is often much greater than other types of memory cards for the same amount of space taken up. Handelman et al disclosed that they would

want to use their invention to store various types of documents and an optical disc would allow for greater amounts of storage.

Handelman et al does not disclose providing the RAM portion which includes user-specific encrypted information which makes the authorizing device unique for a specific user and in combination with the ROM preformed identification signature, provides a user-personalized secure signature. However, RFC 2104 discloses a mechanism for message authentication using a cryptographic hash function and a secret key (Abstract). Further, RFC 2104 states that the keys should be randomly chosen and refreshed or exchanged periodically (section 3). The nature of an optical disc is such that only the RAM portion of the disc can be written and rewritten by a user, so the key can only be stored in the RAM portion of the disc since the key needs to be exchanged periodically. It also makes sense to encrypt the key for security reasons. The key, along with the identification signature already disclosed to exist in the ROM portion of the hybrid disc, would allow for creating a user-personalized secure signature in accordance with the teachings of RFC 2104. One of ordinary skill in the art at the time of the applicant's invention would be motivated to do so because it would allow for the creation of a more secure signature and in case one signature is compromised, a new one can be created easily by the user choosing a new key.

Handelman et al discloses a content supplier downloading selected information to the particular user's memory location (col 4, lines 22-25). Handelman does not disclose the content supplier encrypting the information for each user using the user-personalized secure signature before downloading the information. However, Richards discloses using a communication scheme in which a person would encrypt a message using the key of the person who will be receiving the message before sending the message (col 5, lines 23-33). One of ordinary skill in the art would be motivated to combine the teachings of Handelman et and Richards so that the information downloaded to the user's memory location by the content supplier is first encrypted before being sent because Handelman et al were interested in securing documents so that only authorized users would have access and encrypting such documents before sending them would further secure the documents.

Handelman et al does not disclose a particular user using the user-personalized secure signature to decode such downloaded selected encrypted information each time the user desires to access such information so that after use, only the selected encrypted information remains in the particular user's memory location. However, Richards discloses the user using a personal key to decrypt sent encrypted information (col 5, lines 23-33). Further, given the nature of an optical disc, once an encrypted information has been downloaded onto the disc, the most likely scenario is

that the encrypted information would be further copied into a computer's (or some other device's) memory (RAM) where decryption would occur when a user wishes to access the encrypted information in a usable format. The information on the disc/particular user's memory location would still be encrypted after use. The reason the above mentioned scenario is most likely is that it takes a lot of time to erase and rewrite an optical disc's RAM area, which is the only area on the optical disc the information could be downloaded to, and in the case that one would want to do so to store decrypted information, one would first have to copy the encrypted information off the disc first or else the information would be lost. Once copied, decryption would have to occur off disc anyway. It would be much more time effective to leave the encrypted information on the disc alone and do all decryption off disc.

2. Claim 2: Handelman et al discloses the method of claim 1 wherein the RAM portion of the hybrid optical disc is the user memory location for the downloaded content (col 12, lines 44-54). An optical disc can only consist of two types of memory: a ROM part and a RAM part. As the ROM part can not be written to, it is inherent that any data downloaded must be stored in the RAM part.

Claims 3-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (U.S. 6,298,441) in view of RFC 2104 ("HMAC: Keyed-Hashing for

Message Authentication"), Yamagishi (U.S. 5,379,433), Richards (U.S. 6,385,723), and Wyatt (U.S. 6,041,411).

1. Claims 3 and 9: Handelman et al disclosed a method of transferring information from a content supplier from one or more databases, such information including program(s), audio, still pictures, video, or data files (e.g. lists, spreadsheets, reports, documents, presentation graphics, sales information), or combinations thereof to a location (col 3, lines 9-19) that uses an authorizing hybrid disc that permits the use of such transferred information, comprising the steps of:
    - Providing an authorizing disc having a ROM portion and a RAM portion (col 9, lines 21-27 and col 12, lines 36-54).
    - Providing the ROM portion to include a preformed identification signature which is impressed into the ROM portion of the authorizing disc and is arranged to be difficult for a pirate to copy (col 4, lines 11-21).

The use of hybrid optical discs, which include a RAM and an identification signature located in a ROM portion and is arranged to be difficult for a pirate to copy is also disclosed by Yamagishi (col 2, lines 23-56). One of ordinary skill in the art at the time of the applicant's invention would be motivated to make use of a hybrid optical disc as a smart card because the amount of memory that is available on an optical disc to use as storage for downloaded information is often much greater than other types of memory cards for the

same amount of space taken up. Handelman et al disclosed that they would want to use their invention to store various types of documents and an optical disc would allow for greater amounts of storage.

Handelman et al does not disclose providing the RAM portion which includes user-specific encrypted information which makes the authorizing device unique for a specific user and in combination with the ROM preformed identification signature, provides a user-personalized secure signature. However, RFC 2104 discloses a mechanism for message authentication using a cryptographic hash function and a secret key (Abstract). Further, RFC 2104 states that the keys should be randomly chosen and refreshed or exchanged periodically (section 3). The nature of an optical disc is such that only the RAM portion of the disc can be written and rewritten by a user, so the key can only be stored in the RAM portion of the disc since the key needs to be exchanged periodically. It also makes sense to encrypt the key for security reasons. The key, along with the identification signature already disclosed to exist in the ROM portion of the hybrid disc, would allow for creating a user-personalized secure signature in accordance with the teachings of RFC 2104. One of ordinary skill in the art at the time of the applicant's invention would be motivated to do so because it would allow for the creation of a more secure signature and in case one signature is compromised, a new one can be created easily by the user choosing a new key.

Handelman et al does not disclose a user communicating over a network with the content supplier and selecting information desired to be downloaded. However, Wyatt discloses a system in which digital information is transmitted after a user chooses one or more product over a network (col 5, lines 28-39). One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Handelman et al's teachings with Wyatt's so that only the information the user is interested in is disseminated and no more. As such, the other digital content remain secure with the content provider.

Handelman et al discloses a content supplier downloading selected information to the particular user's memory location (col 4, lines 22-25). Handelman does not disclose the content supplier encrypting the information for each user using the user-personalized secure signature before downloading the information. However, Richards discloses using a communication scheme in which a person would encrypt a message using the key of the person who will be receiving the message before sending the message (col 5, lines 23-33). One of ordinary skill in the art would be motivated to combine the teachings of Handelman et and Richards so that the information downloaded to the user's memory location by the content supplier is first encrypted before being sent because Handelman et al were interested in securing documents so that only authorized users would have access and encrypting such documents before sending them would further secure the documents.

Handelman et al does not disclose a particular user using the user-personalized secure signature to decode such downloaded selected encrypted information each time the user desires to access such information so that after use, only the selected encrypted information remains in the particular user's memory location. However, Richards discloses the user using a personal key to decrypt sent encrypted information (col 5, lines 23-33). Further, given the nature of an optical disc, once an encrypted information has been downloaded onto the disc, the most likely scenario is that the encrypted information would be further copied into a computer's (or some other device's) memory (RAM) where decryption would occur when a user wishes to access the encrypted information in a usable format. The information on the disc/particular user's memory location would still be encrypted after use. The reason the above mentioned scenario is most likely is that it takes a lot of time to erase and rewrite an optical disc's RAM area, which is the only area on the optical disc the information could be downloaded to, and in the case that one would want to do so to store decrypted information, one would first have to copy the encrypted information off the disc first or else the information would be lost. Once copied, decryption would have to occur off disc anyway. It would be much more time effective to leave the encrypted information on the disc alone and do all decryption off disc.

2. Claims 4 and 10: Handelman et al does not disclose a method of claim 3 and method of claim 9 further including the step of a user making payment via the network for the transfer of the selected encrypted information. However, Wyatt discloses an ecommerce system in which payment is made via a network for the selected information (col 6, lines 26-55). One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine the two teachings because many content providers would naturally want to be paid for their contents and Handelman et al disclosed that the content would only be downloaded if the price of the content is within accordance with the user's spending limit (col 3, 2nd paragraph). A payment via a network would be the fastest and most convenient way of rendering payment to the content provider. Further, payment via a credit card over a network has been known at the time of the applicant's invention.
3. Claims 5 and 11: Handelman et al does not disclose a method of claim 4 and a method of claim 10 wherein payment is provided by a user by transferring a payment number which can be used for transferring a predetermined payment amount from a commercial institution that can be for a number of content selections to be selected by the holder of the hybrid optical disc. However, Wyatt discloses entering an account number and a credit card number into an order form so that payment could be rendered for the content selected by a user (col 5, lines 52-56). In the case of Handelman et al, the user is the holder of the hybrid optical disc.

4. Claim 12: Handelman et al does not disclose the method of claim 9 wherein the user-personalized secure signature includes payment authorizing information. However, Wyatt discloses that in one embodiment of his invention, payment information only needs to be entered once and such things as account or credit card number will be stored and associated with the secure signature of the user (col 5, last paragraph). In this manner, the payment authorizing information is the user-personalized secure signature. One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Wyatt and Handelman et al's teachings as it would allow for faster transactions to occur without the user having to enter payment information for each transaction. As such, a content provider would be able to utilize less network resources for each transaction and save on the overhead costs of selling digital content.
5. Claims 6 and 13: Handelman et al disclose the method of claim 3 and the method of claim 9 wherein the RAM portion of the hybrid optical disc is the user memory location for the downloaded content (col 12, lines 44-54).
6. Claims 7 and 14: Handelman et al discloses a method of claim 3 and a method of claim 9 wherein a channel is used to communicate with the remote location via a network and wherein the hybrid disc is encoded with the address of the remote location (col 2, last paragraph; col 3, 1st paragraph; and col 4, lines 26-31).

7. Claims 8 and 15: Handelman et al does not specifically disclose a method of claim 7 and a method of claim 14 wherein the channel is the Internet. However, Wyatt discloses use of the Internet as the channel for communication (col 4, 2nd paragraph). One of ordinary skill in the art would be motivated to use the Internet as the communication channel because it would allow the content providers in Handelman et al's invention to reach a larger population of user more easily and generate more profit.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. Davis et al (U.S. 6,105,008) discloses using a smart card to pay for goods and services.
2. Spies et al (U.S. 6,055,314) discloses a smart card with RAM and ROM portion and use of the public and private key to encrypt and decrypt data.
3. Akiyama et al (U.S. 5,805,699) discloses a method of copying CD's with the use of signatures.
4. Downs et al (U.S. 6,226,618) discloses accessing secure content controlled by a vendor via a network and using a key or signature.
5. Kyer et al (U.S. 5,671,276) discloses encrypting and decrypting packages of services on a network.
6. Mochizuki (U.S. 6,097,814) discloses an optical disk with cipher key.

7. Morales (U.S. 5,291,554) discloses electronic distribution of content over a network and payment system.
8. Tolopka et al (U.S. 6,044,349) discloses a smart card with encrypted identifying data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP